Security Policy: MGEG Secure Card

Worldwide Systems Development Division

Version R01.02.03

Date: April 25, 2003

Repository Information:

Location: /vobs/whirlwind/docs/

Filename: MGEG_FIPS_security_policy

Revision History:

Version #	Date	Author	Description
R01.00.01	12/21/00	Mike French	Initial Revision
R01.00.02	01/24/01	Mike French	Changes made per FTR comments
R01.01.01	06/10/02	Mike French	Upgraded for FIPS 140-2
R01.01.02	09/03/02	Mike French	Updates as per InfoGard representative's suggestions
R01.01.03	09/05/02	Mike French	Added photographs of the MGEG SC.
R01.01.04	09/10/02	Mike French	Added tamper to control input interface.
R01.01.05	10/08/02	Mike French	Added OTAR and programming to interface list.
R01.02.01	10/24/02	Mike French	Final version submitted to InfoGard
R01.02.02	1/10/03	Mike French	Updated Algorithm modes and other minor updates
R01.02.03	4/25/03	Kirk Mathews	Updates per NIST comments

Table of Contents

1. Introduction

1.1. Purpose

This Security Policy is the precise specification of the security rules under which the MGEG Secure Card must operate.

1.2. Scope

This Security Policy specifies the security rules under which the Motorola Gold Elite Gateway Cryptographic Module, herein identified as the MGEG Secure Card or MGEG SC, must operate. Included in these rules are those derived from the security requirements of FIPS 140-2 and additionally, those imposed by Motorola. These rules, in total, define the interrelationship between the:

1. module operators
2. module services
3. security related data items (CSPs).

1.3. Definitions

ALGID		Algorithm Identifier
CBC		Cipher Block Chaining
SC		Secure Card
CFB		Cipher Feedback
CKR		Common Key Reference (interchangeable with SLN)
CO		Crypto Officer
DES		Data Encryption Standard
DPRAM		Dual Port RAM
ECB		Electronic Code Book
KEK		Key Encryption Key
KID		Key Identifier
KLK		Key Loss Key
KMM		Key Management Message
KPK		Key Protection Key
KVL		Key Variable Loader
MAC		Message Authentication Code
MGEG		Motorola Gold Elite Gateway
OFB		Output Feedback
OTAR		Over The Air Rekeying
PRNG		Pseudo Random Number Generator

RNG		Random Number Generator
SLN		Serial Location Number (interchangeable with CKR)
CSP		Security Related Data Item
TEK		Traffic Encryption Key
QUICC		Quad Communications Controller

1.4. Overview

As Motorola radio systems migrate from traditional circuit switched infrastructure to packet based infrastructure, new cryptographic modules are needed to replace those in the current system. X.4 / Astro 6.0 represents the first Astro release to use a packet-based infrastructure. For backwards compatibility, the Motorola Gold Elite Gateway (MGEG), will be released as part of Astro 6.0, so that customers who currently have circuit switched consoles can replace or upgrade their infrastructure without replacing their consoles. The MGEG will be the packet based equivalent of the Digital Interface Unit (DIU). As with the DIU, the MGEG will need to provide voice coding and cryptographic services for the console.

The MGEG Secure Card is a multiprocessor card that can handle up to 120 audio streams providing encryption services for the MGEG. It consists of 1 Motorola MPC8260 Power QUICC II processor, 1 Master Crypto Engine, and 12 Slave Crypto Engines. Each MGEG contains two Secure Cards providing 120 simultaneous, full duplex calls.

1.5. MGEG SC Implementation

The MGEG SC is implemented as a multi-chip embedded module as defined by FIPS PUB 140-2.

1.6. MGEG SC Cryptographic Boundary

The MGEG SC is defined as the portion of the MGEG cPCI printed circuit board containing the following hardware: 13 ARMOR ICs, 1 Flash, 24 SRAMS, 13 DPRAMs, KVL interface and the associated power and tamper circuitry.

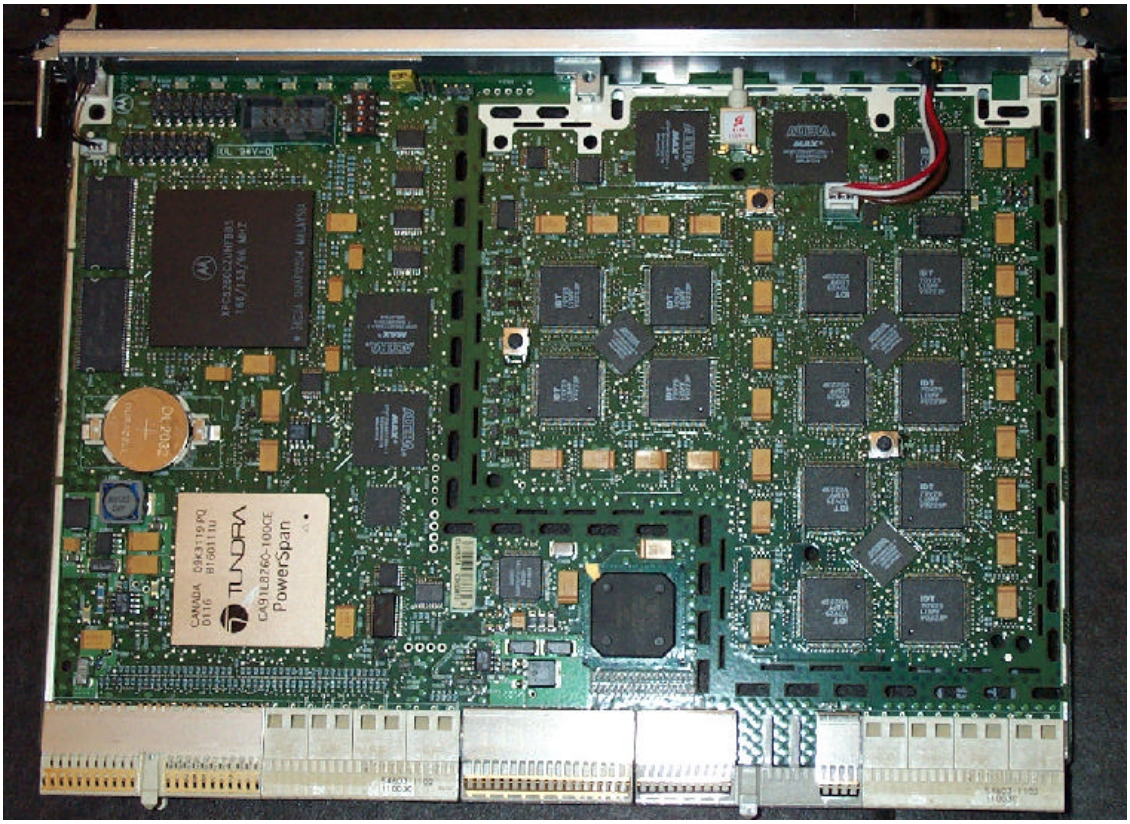

Figure 1: MGEG SC front w/o tamper shield. Crypto boundary defined by dashed 'line'.

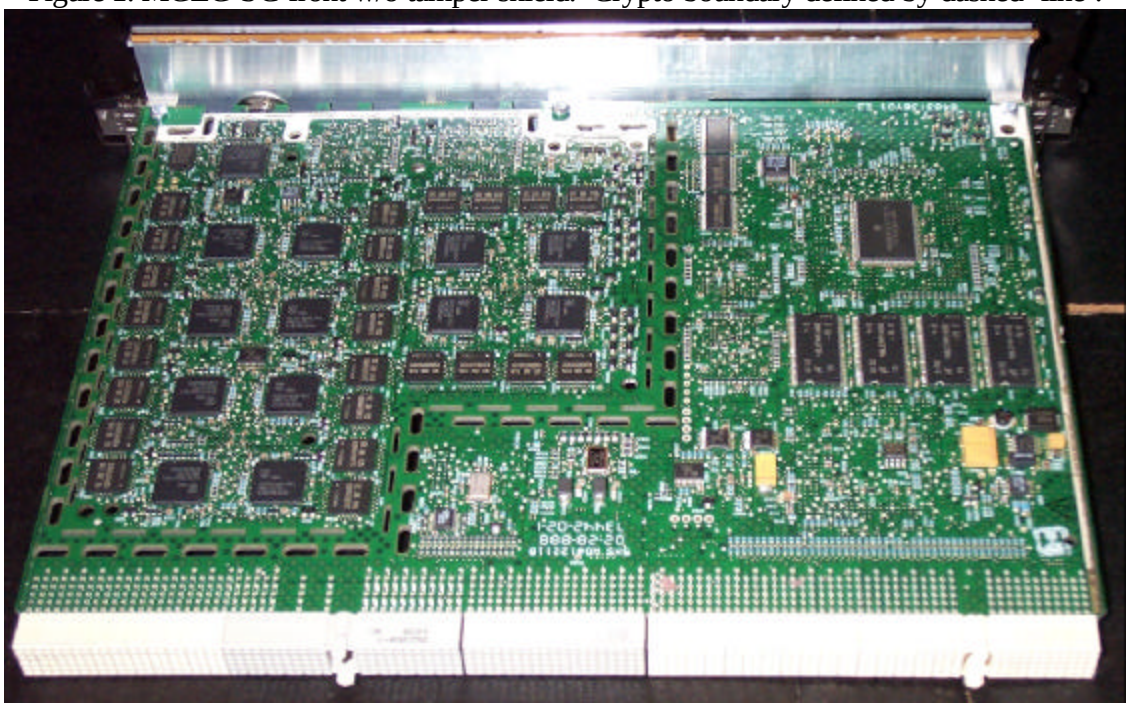

Figure 2: MGEG SC back w/o tamper shield. Crypto boundary defined by dashed 'line'.

NOTE: In the above photographs the tamper shield has been removed to allow the reader to view the internals of the card. The shipped product will include a tamper shield covering both sides of the board that secures to itself through the elliptical holes (appears as a dashed line in the photos) in the board.

2. FIPS 140-2 Security Level

The MGEG SC is designed to meet FIPS 140-2 security at the levels indicated in the table below.

Table 2-1

FIPS 140-2 Security Requirements Section	Level
Cryptographic Module Specification	1
Ports and Interfaces	1
Roles Services and Authentication	2
Finite State Machine Model	1
Physical Security	1
Operational Environment	N/A
Cryptographic Key Management	1
EMI / EMC	1
Self Tests	1
Design Assurance	1
Mitigation of Other Attacks	N/A

3. Approved Operational Modes

The MGEG SC provides modes of operation that are not Approved. Below is a list of configuration settings that are required to provide FIPS 140-2 approved operation. To run the MGEG SC in Approved mode the following three steps must be taken (note: 1 and 2 default to FIPS approved settings at initial power up):

1. Key Loss Key (KLK) generation disabled

2. Tamper mode enabled

3. Algorithms used for encryption, decryption and authentication are as follows:

   DES performed in any of the following modes: ECB, OFB, and CBC

   AES performed in any of the following modes: OFB

4. The following encryption algorithms are *not* FIPS approved: DES-XL, DVI-XL, DVI-SPFL, DVP-XL, SHA-1.

4. Guidance Documentation

4.1. Administration of the MGEG SC in a secure manner (CO)

The MGEG SC can be shipped already installed in the cPCI chassis. In this case, the MGEG SC requires no special administration for secure use assuming settings 1 and 2 in section 3 of this document have not been modified from the default (FIPS approved state) and only FIPS approved encryption algorithms are being used. If the settings have been modified, they must be returned to the FIPS approved state to place the module in FIPS approved mode of operation.

If the Secure Card is sent not installed in the cPCI chassis upon shipment (i.e. MGEG upgrade to secure) the user must install the cards in a secure manner. With the MGEG powered off, the cards must be placed in the cPCI chassis without removing the tamper shield. At initial power up the cards will come up in FIPS approved mode of operation (assuming FIPS approved algorithms are purchased). If parameters 1 and 2 in section 3 of this document are modified, the card is no longer in FIPS approved mode. To return to FIPS approved mode, follow the guidelines in section 3 of this document.

4.2. Assumptions regarding User Behavior (CO)

The MGEG SC has been designed in such a way that very few assumptions regarding User Behavior have been made that are relevant to the secure operation of the module. It has been assumed that the user will keep all CSPs private. It has also been assumed that the user will deny use of the module to unapproved personal while the user is logged in as the User or CO.

4.3. Approved Security Functions, Ports, and Interfaces available to Users

All MGEG SC services are available to the MGEG SC user assuming the appropriate role. These are listed in section 7 of this document.

Only the KVL port (used for electronic key entry and OTAR store and forward) is directly available to the MGEG SC user. This interface is logically disconnected when the user is not logged in with the appropriate role.

4.4. User Responsibilities necessary for Secure Operation

The User and CO must keep all CSPs private. The User and CO must not allow unapproved operation of the module while logged in. The user must ensure the module is operating in the FIPS approved mode as discussed in section 3 of this document.

5. Security Rules

This section lists the security rules enforced by the MGEG SC. The rules are separated into two categories, 5.1) those imposed by FIPS PUB 140-2 and, 5.2) those imposed by Motorola.

5.1. FIPS PUB 140-2 Imposed Security Rules

1. The MGEG SC supports the following interfaces.

   - Data input interface

     a. DPRAM – Plaintext Data, Ciphertext Data, OTAR KMMs

     b. KVL - Key Management Data, Encrypted Cryptographic Keys, Plaintext Cryptographic Keys, OTAR (Store & Forward)

     c. SCI – used to flash program the master crypto engine in the factory

   - Data output interface

     a. DPRAM- - Plaintext Data, Ciphertext Data, OTAR KMMs

   - Control input interface

     a. DPRAM – Input Commands

     b. KVL - Input Commands, Programming Upgrade

     c. Tamper – in addition to the tamper switches beneath the tamper shield, a tamper switch is physically available to the user to cause a tamper response on demand.

   - Status output interface

     a. DPRAM – Status Codes

     b. KVL – Status Codes

     c. KVL LED – KVL interface state

     d. Power up LED – Indicates the MGEG SC is powering up.

   - Power interface

a. SW_3.3 – Switched power supply powers all circuitry except Battery Backed Register

b. CONT_3.3 – Continuous power supply powers Battery Backed Register

2. The MGEG SC inhibits all data output via the data output interface whenever an error state exists and during self-tests.

3. The MGEG SC logically disconnects the output data path from the circuitry and processes when performing key generation, electronic key entry, or key zeroization.

4. Authentication data (e.g. PINs) and other critical security parameters are entered / output in plaintext form.

   AND

   Secret cryptographic keys are entered / output over a physically separate port.

5. The MGEG SC supports a User role and a Cryptographic Officer role. These two roles have the same set of services.

6. The MGEG SC re-authenticates a role when it is powered-up after being powered-off.

7. The MGEG SC provides the following services requiring a role:

   - Zeroize Selected Keys
   - Transfer Key Variable
   - Change Active Keyset
   - Change Password
   - Encrypt
   - Decrypt
   - Privileged APCO OTAR (See section 7.2)

8. The MGEG SC provides the following services not requiring a role:

   - Initiate Self Tests
   - Zeroize all keys
   - Zeroize All Keys and Password

- Reset Crypto Module
- Shutdown Crypto Module
- Receive Log
- Download Config Parameters
- Non-Privileged APCO OTAR (See section 7.2)

9. The MGEG SC enforces Role-Based identification.

10. The MGEG SC implements all software using high-level language except the limited use of low-level language to enhance performance.

11. The MGEG SC protects secret keys and private keys from unauthorized disclosure, modification and substitution.

12. The MGEG SC provides a means to ensure that a key entered into, stored within, or output from the MGEG SC is associated with the correct entities to which the key is assigned. Each key in the MGEG SC is entered and stored with the following information:

    - Key Identifier (KID) – 16 bit identifier
    - Algorithm Identifier (ALGID) – 8 bit identifier
    - Key Type – Traffic Encryption Key or Key Encryption Key
    - Common Key Reference (CKR)/Keyset number – Identifiers indicting storage locations.

    Along with the encrypted key data, this information is stored in a key record that includes a CRC over all of the fields to detect data corruption. When used or deleted the keys are referenced by KID/ALGID or CKR/Keyset.

13. The MGEG SC denies access to plaintext secret and private keys contained within the MGEG SC.

14. The MGEG SC provides the capability to zeroize all plaintext cryptographic keys and other unprotected critical security parameters within the MGEG SC.

15. The MGEG SC supports the following FIPS approved algorithms:

    - DES
      - OFB for symmetric encryption / decryption of digital voice and data
      - CBC for authentication and software upgrades

- ECB for symmetric decryption of Project 25 OTAR

- AES

  - OFB for symmetric encryption / decryption of digital voice and data

  - CBC for MACing of Project 25 OTAR

  - ECB for symmetric decryption of Project 25 OTAR

- 3DES

  - 8-bit CFB for symmetric encryption / decryption of keys and parameters stored in the internal database

16. The MGEG SC performs the following self-tests:

    - Power-up and on-demand tests

      - *Cryptographic Algorithm Test*: Each algorithm is tested using a known key, known data and, if required, known IV. The known, clear data is encrypted with the known key and tested against the known, encrypted data. The encrypted data is then decrypted and tested against the original known clear data. The test passes if both the encrypted and the decrypted known data match their corresponding counterparts, otherwise the test fails.

      - *Software/Firmware Test*: The software firmware test calculates a checksum over the code. The checksum is calculated by summing over the code in 32 bit words. The code is appended with a value that makes the checksum value 0. The test passes if the calculated value is 0, otherwise it fails.

      - *Critical Functions Test:*

        - LFSR Test: The LFSRs are tested by setting the feedback taps to a known value, loading them with known data, shifting the LFSR 64 times, then comparing the LFSR data to a known answer. The test passes if the final data matches, otherwise it fails.

        - General Purpose RAM Test: The general purpose RAM is tested for stuck address lines and stuck bits. This is accomplished through a series of operations that write and read the RAM. The test passes if all values read from the RAM are correct, otherwise it fails.

        - DPRAM Test: The DPRAM is tested for stuck address lines and stuck bits. This is accomplished through a series of operations that write

and read the DPRAM. The test passes if all values read from the DPRAM are correct, otherwise it fails.

Powering the module off then on or resetting the module using the Reset service will initiate the power-up and on-demand self tests.

- Conditional Tests

  - *Software/Firmware Load Test:* A MAC is generated over the code when it is built using DES-CBC. Upon download into the module, the MAC is verified. If the MAC matches the test passes, otherwise it fails.

  - *Continuous Random Number Generator Test:* The continuous random number generator test is performed on 3 RNGs within the module. The first is a hardware RNG which is used to seed the ANSI X9.17 PRNG and the maximal length 64-bit LFSR. The second is an implementation of Appendix C ANSI X9.17 which is used for key generation, and the third is a maximal length 64-bit LFSR which is used for IV generation. For each RNG, an initial value is generated and stored upon power up. This value is not used for anything other than to initialize comparison data. Successive calls to any one of the RNGs generates a new set of data, which is compared to the comparison data. If a match is detected, this test fails, otherwise the new data is stored as the comparison data and returned to the caller.

17. The MGEG SC enters an error state if the Cryptographic Algorithm Test, LFSR Test, Continuous Random Number Generator Test, or the General Purpose RAM Test fails. This error state may be exited by powering the module off then on.

18. The MGEG SC enters a non-fatal error state if the Software/Firmware test fails. This state is exited as soon as an error indicator is output via the status interface and the module enters programming mode.

19. The MGEG SC enters an error state if the Software/Firmware Load test fails. This state is exited as soon as an error indicator is output via the status interface.

20. The MGEG SC outputs an error indicator via the status interface whenever an error state is entered due to a failed self-test.

21. The MGEG SC does not perform any cryptographic functions while in an error state.

5.2. Motorola Imposed Security Rules

The MGEG SC:

1. does not support a bypass mode.
2. does not support multiple concurrent operators.
3. will continue to provide User Role and Crypto Officer Role services until the module has been powered down.
4. will suspend all services during key loading.
5. will zeroize all keys from the Key Database after a sufficient number (15) of consecutive, unsuccessful user login attempts.
6. shall erase all plaintext keys upon detection of a critically low voltage on the switched (SW_3.3) power supply.
7. shall erase all security related data items (CSPs, see section 9.1) upon detection of a critically low voltage condition on both the switched (SW_3.3) and continuous (CONT_3.3) power supply.
8. shall erase all CSPs upon detection of tamper.
9. shall at no time output any CSPs.

6. Physical Security

6.1. Mechanisms

The MGEG SC uses two tamper switches beneath a hard metal tamper shield for tamper detection. When the tamper shield is removed the switch(s) open(s) and a tamper response results. There is an third tamper switch that is user accessible for intentional erasure of CSPs.

6.2. Maintenance

No maintenance is required to ensure physical security.

7. Roles and Services

7.1. MGEG SC Supported Roles

The MGEG SC supports two (2) roles:

- User Role
- Crypto Officer (CO) Role

7.2. MGEG SC Services

- Transfer Key Variable: Transfer Key variables to the Key Data Base (KDB) via a Key Variable Loader (KVL) or zeroize key variables from the KDB via a KVL. Avaliable to User and CO roles Service input: KMM. Service output: KMM.
- Change Password: Modify the current password used to identify and authenticate the User and CO Roles. Available to User and CO Roles. . Service input: DPRAM message (opcode; old password; new password). Service output: DPRAM message (opcode; status).
- Validate Password: Provides a method of controlling use of CSPs. Available to all roles. Service Input: DPRAM message.
- Encrypt Digital: Encrypt digital voice or data. Available to User and CO Roles. Service input: DPRAM message (opcode, red data). Service output: DPRAM message (opcode, black data, status).
- Decrypt Digital: Decrypt digital voice or data. Available to User and CO Roles. Service input: DPRAM message (opcode, black data). Service output: DPRAM message (opcode, red data, status).
- Initiate Self Tests: Performs module self tests comprised of cryptographic algorithms test, software firmware test, and critical functions test. Initiated by module reset or transition from power off state to power on state. Available without a Role. Service input: power applied. Service output: DPRAM message (opcode).
- Privileged APCO OTAR: Modify and query the Key Database via APCO OTAR Key Management Messages (KMMs). Available to User and CO Roles. Service input: KMM. Service output: KMM.
- Zeroize Selected Keys: Zeroize selected key variables from the Key Database by Common Key Reference (CKR). Available to User and CO Roles. Service input: KMM. Service output: KMM.

- Zeroize all keys: Zeroize all keys from the Key Database. Available without a Role. (Module can be reinitialized using KVL). Service input: KMM. Service output: KMM.

- Zeroize All Keys and Password: Zeroizes all keys and CSPs in the key database. Resets the password to the factory default. Allows user to gain controlled access to the module if the password is forgotten. Available without a Role. (Module can be reinitialized using KVL). Service input: 15 consecutive Failed Passsword Validation attempts.

- Tamper Response: Erases all CSP's with the exception of the password upon detection of tamper. Service Input: Hardware Tamper switch.

- Non-Privileged APCO OTAR: Hello and Capabilities KMMs may be performed without a Role. Service input: KMM. Service output: KMM.

- Reset Crypto Module: Soft reset of module to remove module from error states. Available without a Role. Service input: DPRAM message (opcode). Service output: DPRAM message (opcode).

- Shutdown Crypto Module: Prepares module for removal of power. Available without a Role. Service input: DPRAM message (opcode). Service output: DPRAM message (opcode).

- Download Configuration Parameters: Download configuration parameters used to specify module behavior. For example enable / disable APCO OTAR etc. Modification of some security related parameters (single key mode, tamper mode) causes key erasure. Available without a Role. Service input: DPRAM message (opcode, parameter ID, parameter value). Service output: DPRAM message (opcode, parameter ID, parameter status).

- Programming Upgrade: Allows users to upgrade CE software. Service Input: Programming messages via the KVL.

8. Authentication

The MGEG SC uses a 40-bit password to implicitly authenticate the User and CO roles. The password is initialized to a default value during manufacturing. After authenticating, the password may be changed at any time. Fifteen consecutive invalid authentication attempts erases all keys from the Key Database.

9. Access Control

9.1. Security Related Data Items (CSPs)

Table 9-1

CSP Identifier	Description
Key Protection Key (KPK)	Key used to encrypt the database and other non-volatile parameters
Plaintext Traffic Encryption Keys (TEKs)	Keys used for voice and data encryption
Plaintext Key Encryption Keys	Keys used for encryption of keys in OTAR
Plaintext MAC Key	Key used for authentication of software upgrade. Stored in non-volatile memory
Plaintext Password	Operator password entered during user authentication

9.2. CSP Access Types

Table 9-2

CSP Access Type	Description
Retrieve key	Decrypts encrypted TEKs or KEKs in the database using the KPK and returns plaintext version
Store key	Encypts plaintext TEKs or KEKs using the KPK and stores the encrypted version in the database
Erase Key	Marks encrypted TEK or KEK data in key database as invalid
Create KPK	Generates and stores new KPK
Store Password	Hashes user password and stores it in the database

9.3. Access Matrix

	CSP Access Operation					Applicable Role		
User Service	Retrieve Key	Store Key	Erase Key	Create KPK	Store Password	User Role	Crypto Officer Role	No Role Required
1. Transfer Key Variable		X	X			X	X	
2. Privileged APCO OTAR	X	X	X			X	X	
3. Validate Password						X	X	X
4. Change Password			X	X	X	X	X	
5. Encrypt	X					X	X	
6. Decrypt	X					X	X	
7. Initiate Self Tests						X	X	X
8. Zeroize Selected Keys			X			X	X	
9. Zeroize All Keys			X			X	X	
10. Zeroize All Keys and Password			X		X	X	X	
11. Tamper Response			X			X	X	X
12. Non-Privileged APCO OTAR						X	X	X
13. Reset						X	X	X
14. Shutdown						X	X	X
15. Download Config Parameters			X	X		X	X	
16. Programming Upgrade						X	X	

10. Mitigation of Attacks

The MGEG SC does not mitigate any attacks that are not defined in the FIPS 140-2 standard.